January 13, 2016 Meeting Minutes

Meeting commenced 8:00PM GMT

- Roll call (Valerie)
- Quorum achieved

Proposed agenda

- V2.40
  - Errata process update
- V2.41
  - Next Steps
- V3.0
  - any discussion
- Face to face
- Interop update
- Topics for next call
- New Business
- Review Action Items
- Adjourn

Motion to approve Agenda

- Tim Moves, Chris Seconds, no objections, no abstentions. Agenda approved

Motion to approve meeting minutes

- Minutes completed but not posted - deferred to the next meeting.
- See https://wiki.oasis-open.org/pkcs11/Meetingminutes/Minutes09122015

v2.40

Errata process update

- Dina - her comments on TLS may have been addressed in the v2.40 errata by Tim/BobG

- Action: revisit this in v2.41 to see what additional changes we need to make around TLS.

v2.41

Next Steps

- Valerie would like to consider adding SHA3. Tim concurs.
- Valerie. ChaCha20 and Poly - should also be included. BobR agrees.

New mechanisms

- Handling new mechanisms. What did we discuss?
- Tim - we discussed this as a separate document and take to committee note draft and then wrap into next spec or at least have it as committee draft.
- Looking for volunteers to write up SHA3 - BobR action item; and Chacha and Poly - pending.

Dina: TLS 1.X text improvements

- Pending - include as topic next

AES GCM

- This is important to sort out for a pending validation update for RedHat - so BobR wants to include this in v2.41.
- Wan-Teh's proposal isn't exactly a v2.41 approach - needs new functions - added in a way that would work for v3.0 - sort of a v3.0 "lite".
- The FIPS140-2 IV's must be generated externally. This new IG is an issue.

NIST CMVP feedback

- BobR plans to provide feedback through labs on the issue of changes and their impact on vendors.
- Valerie also provided rather direct feedback to NIST people at ICMC.
- How do we submit this? Tim suggested a comment with a motion from the TC for a member to submit on behalf of the TC.
- BobR will work on the wording for this for the next call.

V3.0

- Nothing more on this topic outside the items already mentioned under v2.41

Face to Face - 26th Feb

- BobR thinks that RedHat can host - still waiting on internal approvals but thinks this is on track.
- Tim - can apply to idTrust for funding for dinner.
- Valerie will send email to Saikat&Tony about coordinating dates and the process for applying to idTrust for funding.
- Tim suggested also checking with Bruce Rich as he was until recently on the idTrust committee so he knows how that works.

Interop update

- Tim provided an update - progressing well.
- Valerie - we had update from Jane. Note longer expo show hours.

Next meeting date

- 27th January 2016

Next meeting proposed agenda

- F2F organisation around RSA2016

New Topic

- Dina raised issue on HMAC general mechanism. Signature length of 0 is meaningless. We will need to clean this up.
- Open action item. Tony to file to Jira.

Action Items

- See Jira - https://issues.oasis-open.org/browse/PKCS/?selectedTab=com.atlassian.jira.jira-projects-plugin:issues-panel
- Will review action items at next meeting.

Call for late arrivals

- None

Motion to Adjourn

- Tim Moves, Greg seconds, no abstentions, no objections. Motion approved

Meeting Adjourned at 8:33PM GMT

Meetingminutes/Minutes13012016 (last edited 2016-01-27 20:20:23 by bubbva)